SOBRE LA MESA *(FOOD FOR THOUGTH)*

UN ANÁLISIS PERIÓDICO DE LOS PRINCIPALES PROBLEMAS Y TENDENCIAS DE LA PRÁCTICA DE MARSH EN LA INDUSTRIA DE ALIMENTOS Y BEBIDAS

GESTIÓN DE LOS CRECIENTES RIESGOS CIBERNÉTICOS EN LAS EMPRESAS DE ALIMENTOS Y BEBIDAS

Generalmente se considera al riesgo cibernético como sinónimo de filtración de información. Pero para las empresas de alimentos y bebidas, la alteración de las operaciones normales a partir de un fallo tecnológico representa una amenaza potencial aún mayor. Ninguna empresa de alimentos y bebidas puede erradicar esta amenaza por completo, pero las organizaciones pueden tomar medidas para minimizar la pérdida de ingresos, el daño a su reputación y otros efectos adversos generados por dichas alteraciones.

LOS ATACANTES CIBERNÉTICOS EXTIENDEN SU ALCANCE

Imagine que uno de sus empleados revisa su correo electrónico empresarial y se encuentra con un mensaje que parece ser de un proveedor confiable. El empleado hace clic en un enlace del correo, y su computadora se congela. Aparece un mensaje: “Sus archivos fueron encriptados. Pague el rescate dentro de 24 horas a cambio de la clave para desencriptar sus archivos”. Si usted no paga, sus datos serán destruidos o simplemente no podrá acceder a ellos debido al software malicioso de encriptado.

Los ataques de este tipo son conocidos como ransomware (secuestro de información), una forma de malware que los criminales cibernéticos usan cada vez más para extorsionar a personas y negocios a cambio de dinero. Esto es tan solo un ejemplo de cómo han evolucionado los ciberataques.

Durante la última década, las empresas se han vuelto progresivamente más dependientes de la tecnología. Los fabricantes y procesadores de alimentos y bebidas, por ejemplo, utilizan computadoras para manejar sus líneas de producción y monitorear el movimiento de los productos e ingredientes a través del proceso de producción. Por otro lado, los restaurantes suelen depender de la tecnología para gestionar las transacciones con los clientes, las reservaciones, el inventario y otras funciones esenciales.

Al mismo tiempo, los atacantes cibernéticos se han vuelto más sofisticados y han extendido su alcance. Los criminales siguen buscando oportunidades de robar la información de identificación personal de los clientes. Aunque algunos sectores de la industria de alimentos y bebidas siguen enfrentando estas amenazas –más notablemente, los restaurantes– los atacantes cibernéticos actualmente también tienen como objetivo a las empresas y buscan oportunidades para extorsionar y pedir dinero u obtener algún otro beneficio mediante la alteración de tecnologías.

Las pérdidas potenciales pueden llegar a ser enormes para las empresas de alimentos y bebidas que son víctimas de dichos ciberataques. Estas pérdidas incluyen daños, corrupción o pérdida de datos; gastos adicionales para reemplazar o reparar los equipos tecnológicos y de cómputo averiados; y lucro cesante –incluyendo la pérdida de utilidades– en caso de que sean alterados sistemas esenciales.

CUANTIFICACIÓN DEL RIESGO CIBERNÉTICO DE LUCRO CESANTE

Para gestionar las pérdidas directas ocasionadas por un ciberataque, incluyendo lucro cesante (LC), el primer paso es estimar el impacto financiero

potencial. Cada evento de LC cibernético es distinto, dependiendo de detalles específicos como el modelo de negocios de la organización y su modo de respuesta. Mediante el uso de un análisis basado en escenarios para cuantificar el riesgo cibernético de LC, una empresa puede determinar un patrón de hechos hipotéticos y estimar los costos resultantes. Un análisis basado en escenarios debe enfocarse en tres factores:

- **Estimar la probabilidad y gravedad de un evento de LC cibernético.** Los riesgos cibernéticos por lo general se han clasificado simplemente como riesgo elevado, medio o bajo, pero este método suele tener un valor limitado. En su lugar, los riesgos de LC cibernético pueden expresarse de forma cuantitativa: ¿Cuál es la probabilidad de que una organización sufra una interrupción dentro de un periodo específico y qué tan graves pueden ser las pérdidas?

- **Identificar las opciones de mitigación.** Dependiendo de la magnitud de la exposición de una organización al LC cibernético, las opciones pueden incluir cambiar los procesos de negocios, actualizar la infraestructura de TI para mejorar su resiliencia, mejorar las capacidades de recuperación o fortalecer los controles técnicos de ciberseguridad. Es importante contar con una estimación creíble de la exposición potencial al LC cibernético a fin de evaluar adecuadamente estas decisiones e identificar las estrategias que tendrán el mayor impacto.

- **Evaluar las opciones de transferencia del riesgo.** Son muchas las empresas que no cuantifican sus riesgos por completo antes de verse afectadas por un siniestro, lo cual significa que el LC cibernético con frecuencia se encuentra insuficientemente asegurado o no asegurado. Sin embargo, las aseguradoras de daños patrimoniales tradicionales y cibernéticos ofrecen coberturas cada vez más amplias para esto riesgos. La cuantificación de los riegos cibernéticos de lucro cesante es crucial para la toma de decisiones en términos de contratación de límites y otros datos específicos de las pólizas.

MITIGACIÓN DEL RIESGO

Después de la cuantificación, los negocios pueden tomar acciones para mitigar el riesgo cibernético de LC. Las empresas de alimentos y bebidas deben considerar varias medidas para estar mejor protegidas ante el impacto potencial de un ransomware, así como de otros ciberataques directos, incluyendo:

- **Respaldar archivos.** Muchos negocios no respaldan sus archivos con regularidad en un sistema independiente. Tener la capacidad de recuperar sus datos puede hacer que perder el acceso a una fuente de información sea sustancialmente menos perjudicial.

- **Mantener el software actualizado.** Como parte de una estrategia general de prevención de riesgos cibernéticos, los administradores de TI deben asegurarse de que los sistemas operativos, software antivirus y navegadores de internet se actualicen con regularidad. También deben aplicarse configuraciones de seguridad en los navegadores de internet –por ejemplo, para bloquear anuncios emergentes y plug-ins potencialmente vulnerables–.

- **Capacitar a los empleados.** Los departamentos de TI deben mantenerse informados acerca de las más recientes herramientas y técnicas usadas por los criminales cibernéticos. Los profesionales de riesgos también deben recordar que la línea de defensa más efectiva contra el ransomware y otras amenazas es un usuario informado. Los empleados deben estar capacitados para detectar correos electrónicos potencialmente peligrosos y para no abrir archivos adjuntos ni hacer clic en enlaces de correos no solicitados –incluyendo aquellos que aparentemente son de proveedores, distribuidores y otras fuentes confiables–.

- **Practicar la respuesta.** Antes de que ocurra un ataque, las empresas deben crear planes de respuesta ante incidentes. Estos planes deben ser puestos a prueba mediante ejercicios teóricos, utilizando incidentes cibernéticos hipotéticos que sean realistas para su empresa. Esto puede ayudar a identificar las áreas por mejorar o que deben revisarse.

COBERTURA DEL SEGURO

Los seguros de daños patrimoniales normalmente excluyen la cobertura para eventos cibernéticos; estas pólizas tradicionalmente responden únicamente ante pérdidas físicas. No obstante, debido a que las empresas sufren cada vez más eventos de lucro cesante a causa de ransomware u otras formas de ciberataques que no implican daños físicos, las aseguradoras de daños patrimoniales parecen cada vez más abiertas a proporcionar cobertura en estos casos. Algunas de las principales aseguradoras de daños patrimoniales han expresado recientemente que sus pólizas cubrirán eventos cibernéticos especificados de primeras partes. Otras aseguradoras de daños patrimoniales podrían admitir una cobertura similar en sus pólizas, usualmente mediante un endoso y caso por caso.

Mientras tanto, las pólizas cibernéticas independientes siguen evolucionando. Cuando las pólizas de cobertura cibernética fueron desarrolladas inicialmente, éstas se enfocaban principalmente en ataques de hacking contra sitios web corporativos. Pero actualmente las pólizas cibernéticas normalmente cubren una amplia gama de riesgos generados por:

- La manipulación o recopilación de información confidencial.

- La dependencia de las operaciones en la tecnología.

Por consiguiente, las pólizas actuales pueden cubrir los fallos tecnológicos y la resultante interrupción o pérdida de utilidades –independientemente de la causa inicial–. Asimismo, las aseguradoras están reconociendo cada vez más la interdependencia de los negocios, especialmente con respecto a la tecnología, y normalmente están dispuestas a incluir lucro cesante contingente (LCC) en sus pólizas cibernéticas. Una póliza cibernética también puede cubrir eventos que ocasionen daños patrimoniales; por ejemplo, daño a una computadora o servidor. Sin embargo, las pólizas cibernéticas no suelen tener como objetivo cubrir fallos tecnológicos derivados de eventos físicos, por ejemplo, derrumbe de edificios, inundaciones, incendios u otros riesgos físicos.

Conforme se desarrollan programas de aseguramiento para cubrir toda una gama de potenciales riesgos cibernéticos, es importante que las empresas de alimentos y bebidas coordinen sus decisiones al adquirir seguros contra riesgos cibernéticos, de daños patrimoniales y de responsabilidad civil. Los profesionales de riesgos deben colaborar con sus asesores de seguros para realizar un diagnóstico de estas pólizas a fin de determinar los niveles actuales de cobertura, identificar toda brecha o exclusión, y desarrollar estrategias para una mejor gestión de los riesgos cibernéticos de sus organizaciones.

Este resumen fue elaborado por Marsh's Food & Beverage Practice, en colaboración con Marsh's Cyber Practice y Marsh Risk Consulting.

Para más información acerca de este tema, póngase en contacto con su representante local de Marsh.